1. A method of exchanging a cryptographic key between two users, comprising the steps of:

a) each of said two users selecting a value p from the group of equations consisting of:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (*mod* 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$

b) each of said two users selecting an elliptic curve E and an order q;

c) each of said two users selecting a base point $G=(G_x, G_y)$ on the elliptic curve E, where G is of order q;

d) each of said two users generating a private key w, where w is an integer;

e) each of said two users generating a public key $W=wG$, where W is the corresponding user's public key, where w is the corresponding user's private key, and where G is the corresponding user's basepoint;

f) each of said two users distributing their p, E, q, G, and W in an authentic manner;

g) the two users agreeing on p, E, q, G, W_1, and W_2, where W_1 is the public key of one of said two users, and where W_2 is the public key of the other of said two users;

h) each of said two users generating a private integer;

i) each of said two users multiplying G by each of said user's private integer generated in the last step using a form of p agreed upon;

j) each of said two user transmitting the result of the last step to the other of said two users;

k) each of said two users combining one of said two user's private integer and public key with the other of said two user's result of step (j) and public key using the form of p agreed upon to form a common secret point between each of said two users; and

l) each of said two users deriving the cryptographic key from the common secret point.